

2019-2020

商用密码行业分析报告

2021年2月

参与评审单位:(排名不分先后)

深圳市商用密码行业协会

北京安御道合科技有限公司

北京海泰方圆科技股份有限公司

北京数盾信息科技有限公司

云上(江西)密码服务科技有限公司

江南信安(北京)科技有限公司

北京三未信安科技发展有限公司

北京数字认证股份有限公司

商密在线(北京)科技有限公司



VISIT...

LANZAROTE
Caliente.COM

目录

- 1 中国商用密码产业概况
- 2 中国商用密码市场分析
- 3 中国商用密码产业链分析



1

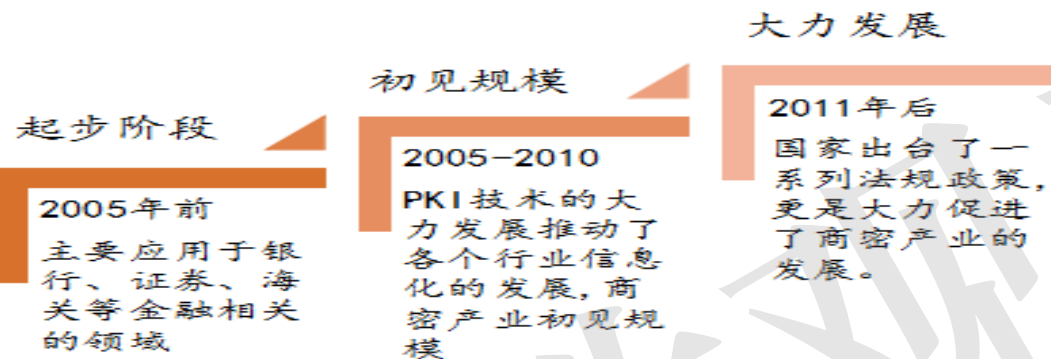
中国商用密码产业概况

发展历程



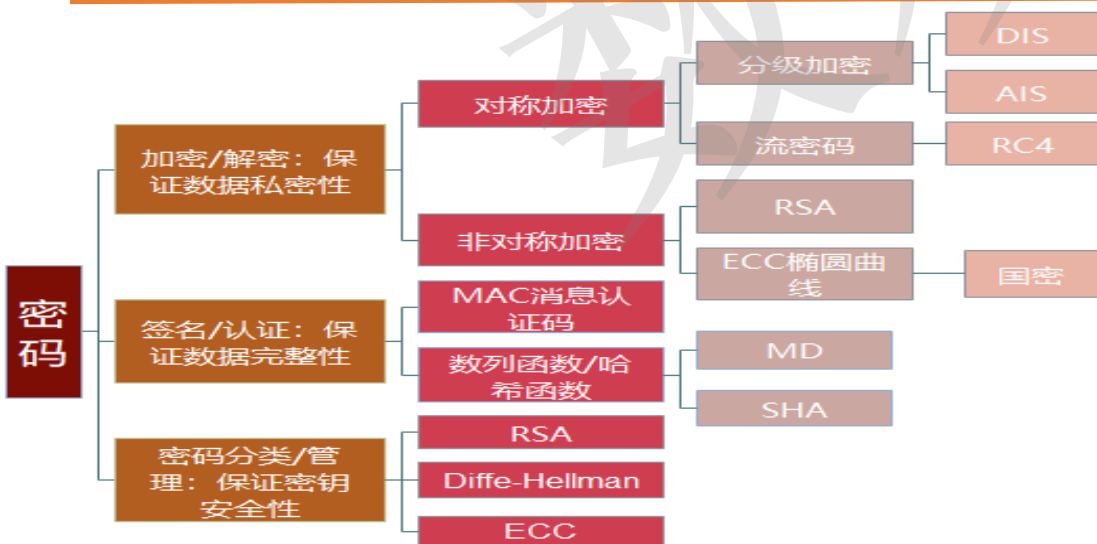
我国真正意义上的商密行业只有二十多年的发展历史，其发展轨迹大致可分为以下三个阶段：

起步阶段（2005 年之前）：主要应用于银行、证券、海关等金融相关的领域. 金融行业的监管要求推动了金融数据密码机等商密产品的研制及应用。



初见规模（2005-2010年）：基于数字证书的PKI 技术(公钥密码基础设施)取得大力发展，商用密码产品和技术为网络上的身份认证、数据传输加密、电子签名等提供技术支撑，推动了电子商务、电子政务、各个行业信息化的发展，我国的商密产业初见规模。

密码分类



大力发展（2011年以后）：2011年，密码行业标准化技术委员会正式成立，制定了SM2/3/4/9、ZUC等密码算法标准以及一系列密码协议、产品等行业标准，逐渐建立了我国的商用密码标准体系。近几年，国家出台了一系列法规政策，更是大力促进了商密产业的发展。



本行业有着特殊的信息安全要求，同时受到信息产业和安全主管部门的监管。相关主管部门及其职责如下：

主管部门	主要职责
中央网信办	着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题；研究制定网络安全和信息化发展战略、宏观规划和重大政策；推动国家网络安全和信息化法治建设，不断增强信息安全保障能力。
国家发展和改革委员会、工业和信息化部	负责产业政策的研究制定、行业的管理与规划等
公安部	主管全国公共信息网络的安全监察工作、网络信息安全及等级保护的监督管理工作和网络信息安全产品的销售许可工作等。
国家密码管理局商用密码管理办公室	主管全国商用密码管理工作，批准生产的商用密码产品品种等
国家保密局	管理和指导保密技术工作，负责办公自动化和计算机信息系统的保密管理，指导保密技术产品的研制和开发应用，多从事涉密信息系统集成的企业资质进行认定。
国家知识产权局	负责组织协调全国知识产权保护工作，推动知识产权保护工作体系建设。
中国信息产业商会	组织行业内企业开展各项活动和内部交流；发起分类安全标准的起草工作、研究抵制安全行业市场内的不正当竞争、组织跨行业的安全大会；引导会员认真执行国家的法规和政策、遵守行规、行约等。



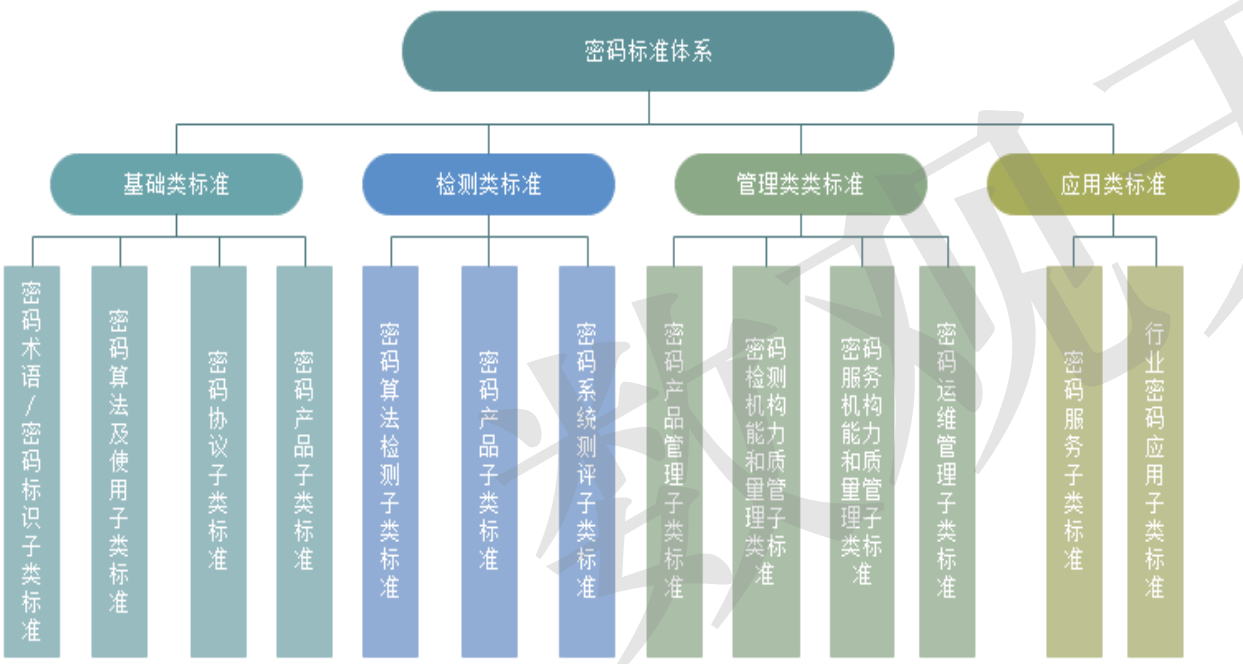
目前，国内商用密码行业相关的主要法律法规如下：

时间	发文单位	文件名称	相关内容概要
1999年10月	国务院	《商用密码管理条例》	是我国商用密码领域第一个行政法规，标志着我国商用密码的发展和管理从此走上了法治化的轨道。
2003年9月	中办国办	《关于加强信息安全保障工作的意见》	第一次明确了密码在信息安全保障工作中的基础性地位和关键作用。
2004年8月 (2019年修正)	全国人大常委会	《中华人民共和国电子签名法》	是电子认证服务业的根本法律，是我国第一次从法律上确定了可靠的电子签名与手写签名或者盖章具有同等的法律效力。
2005年12月	国家密码管理局	《商用密码产品生产管理规定》	规定了商用密码产品由国密局指定的单位生产。
2005年12月 (2017年修正)	国家密码管理局	《商用密码科研管理规定》	规定了商用密码的科研承担对象以及科研成果的验收流程。
2009年10月 (2017年修正)	国家密码管理局	《电子认证服务密码管理办法》	规定电子认证服务提供者提供电子认证服务必须申请《电子认证服务使用密码许可证》。
2010年4月	全国人大常委会	《中华人民共和国保守国家秘密法》	规定了国家秘密的秘级，保密制度和相关法律责任
2016年11月	全国人大常委会	《中华人民共和国网络安全法》	制定网络安全战略，明确网络空间治理目标，强化了网络运行安全，同时也将催生不断扩大的网络安全市场空间，产业投入和建设也将步入持续稳定的发展轨道。
2019年10月	全国人大常委会	《中华人民共和国密码法》	其中密码法第三章商用密码部分，规定了商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度。



行业标准

//



密码标准体系框架

01

当前，商用密码的行业标准分为基础类标准、应用类标准、检测类标准和管理类标准。

02

基础类标准为其他三类标准提供了底层、共性支撑（如术语、算法、协议、产品等）；

03

检测类标准为基础类标准和应用类标准提供了合法性检测的功能，保障商用密码使用的合法性；

04

管理类标准为其他三类标准提供了管理功能；

05

应用类标准为上层具体的密码产品、服务应用提供支持。



01

国家主席习近平10月26日签署了第35号主席令：《中华人民共和国密码法》已由中华人民共和国第十三届全国人民代表大会常务委员会第十四次会议于2019年10月26日通过，现予公布，自2020年1月1日起施行。

密码的分类与管理

- 密码法将密码分类为核心密码、普通密码与商用密码，并要求对这三类密码实行分类管理。
- 其中“核心密码”与“普通密码”被用来保护国家秘密信息，涉密单位应重点关注对于这两类密码的管理。对这两类密码，《密码法》要求实行密码“保密责任制”和“安全风险评估”机制。
- 而商用密码被用于保护不属于国家秘密的信息，公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。一般来说非涉密单位接触到的密码应用，都属于商用密码，应遵循国家密码局商用密码管理有关条例规定。

02

03

密码安全性评估成为必须

- 本次《密码法》发布对于非涉密的企事业单位来说，最大的影响就是必须要主动进行“密码安全性评估”。
- 根据《密码法》要求，商用密码产品及服务使用方应按照国家密码管理局有关规定，对商用密码产品、密码服务、密码技术进行安全性以及合规性认证。
- 并对关键信息基础设施，应采用商用密码进行保护，并进行密码安全性评估，同时与关键信息基础设施安全检测评估、网络安全等级测评制度密码相关要求相衔接。

《密码法》主要内容

《密码法》共五章四十四条，重点规范了以下内容：

第一章总则部分，规定了本法的立法目的、密码工作的基本原则、领导和管理体制，以及密码发展促进和保障措施。

第二章核心密码、普通密码部分，规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施。

第三章商用密码部分，规定了商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度。

第四章法律责任部分，规定了违反本法相关规定应当承担的相应的法律后果。

第五章附则部分，规定了国家密码管理部门的规章制定权，解放军和武警部队密码立法事宜以及本法的施行日期。

04



产业影响因素

产业特点

01

周期性：客户主要分布于政府和国家重点行业，收入来源中政府预算支出和重点行业客户支出占比较高，受一定宏观经济影响，是偏向于弱周期性的行业。

02

季节性：政府、金融、电信、能源等国家重点行业通常采取预算管理制度和集中采购制度，上半年审批上一年度预算和投资采购计划，下半年进行项目招标采购，因此行业呈现季节性特征，上半年销售订单较少，从年度中期开始增多，第四季度达到产品销售和交付的高峰。

03

地域性：受区域经济情况，政策辐射效力、重点行业单位数量、企业数量等因素影响，华东、华北、华南区域市场份额占比较高。

04

行业性：受国家政策、自身需求等因素影响，政府和国家重点行业客户一直是产业发展的主要推动力量。

影响因素

● 网络攻击日益频繁

随着身份盗用、交易诈骗、资源滥用、网络钓鱼等安全事件频繁发生，政府、企业、个人对信息安全的关注程度日益增强，社会对信息安全的需求与日俱增，政府部门、重点行业在信息安全产品和服务上的投入也不断增加，促进了信息安全行业的持续增长。

● 合规要求趋严

2017-2019年，随着《网络安全法》、《央企考核办法》、《等保2.0》、《数据安全》、《产业规划》、《密码法》等的陆续出台，叠加HW行动、信创等政策因素，网安相关政策的影响力持续加强，合规需求仍是现阶段行业主题。

● 信息技术不断发展革新

近年来，云计算、大数据、移动以及社交网络的快速发展给信息系统架构带来了巨大变化，信息安全也随之迎来挑战。例如云计算技术，使得数据中心的基础设施由原来的各业务系统独立建设模式转变为资源池建设模式，服务器、存储、网络设备的部署方式相应改变。基础架构的变化要求信息安全建设能够适应新的IT基础架构，从而满足新的安全需求，这同时为信息安全建设带来了新的发展空间。

● 产品推广周期较长

由于信息安全行业的特殊性，行业内企业不但要具备相应信息安全企业资质，并且新技术、新产品需要经过公安部、密码管理局、国家信息安全认证中心等众多部门审批合格后方可推向市场，一定程度上限制了行业技术革新以及产业化推进。

密码产品检测机构

更多资料，欢迎访问 www.wenku120.com

See
Data



密码管理局

国家密码管理局商用密码检测中心

国家密码管理局全称为国家商用密码管理办公室，国家密码管理局位于北京市丰台区。

组织贯彻落实党和国家关于密码工作的方针、政策，研究提出解决密码工作发展中重大问题的建议；拟订密码工作发展规划，起草密码工作法规并负责密码法规的解释，组织拟订密码相关标准；依法履行密码行政管理职能，管理密码科研、生产、装备（销售），测评认证及使用，查处密码失泄密事件和违法违规研制、使用密码行为，负责有关密码的涉外事宜。



鼎铉密码

鼎铉商用密码测评技术（深圳）有限公司

鼎铉商用密码测评技术（深圳）有限公司（下称“鼎铉公司”）成立于2017年3月，是国家密码管理局授权的全国性第三方商用密码检测机构，也是中国密码学会密码测评专委会及区块链专委会发起创建单位、区块链密码创新联盟理事长单位、广东省商用密码协会监事长单位、深圳市商用密码行业协会会长单位。2019年，公司获评为国家高新技术企业；2020年，被认定为“广东省密码产品与系统测评工程技术研究中心”



智巡密码

智巡密码（上海）检测技术有限公司

智巡密码（上海）检测技术有限公司（以下简称“智巡”）于2018年8月在上海市松江区泗泾镇创办。智巡承担上海市第三方商用密码检测机构培育工作的建设，具备国家商用密码产品检测资质和商用密码应用安全性评估试点资质，是G60商用密码产业和应用示范基地的核心功能平台，也是上海市商用密码行业协会和长三角G60科创走廊智慧安防产业联盟的发起单位。



豪符密码

豪符密码检测技术（成都）有限责任公司

国有控股企业，国家密码管理局授权建设的第三方商用密码检测机构，2019年底被列入四川省委省政府信息技术应用创新产业重大项目。豪符公司立足四川、重点面向中西部提供商用密码及网络安全产品技术检测，商用密码及网络空间应用安全检测，研制生产先进的密码检测系统装备，提供相应技术服务及培训服务，以此进一步推进密码科技创新产业园的建设与发展。



密码测评机构

(排名不分先后)

第一批

- 智巡密码（上海）检测技术有限公司
- 国家信息技术安全研究中心
- 深圳市网安计算机安全检测技术有限公司
- 河南中科安永科技有限公司
- 江苏省信息安全测评中心
- 中国电子科技集团15所
- 公安部第三研究所
- 中国金融电子化公司
- 北京银联金卡科技有限公司
- 工业和信息化部电子第五研究所
- 中国科学院数据与通信保护研究中心
- 国家密码管理局商用密码检测中心

第一批

- 教育部教育管理信息中心
- 国家广播总局广播电视科技研究院
- 长春市博鸿科技服务有限公司
- 安徽科测信息技术有限公司
- 山东道普测评技术研究中心
- 国电南京自动化股份有限公司
- 北京市电子产品质量检测中心
- 浙江东安检测技术有限公司
- 交通运输部信息安全中心有限公司
- 成都市信息系统与软件测评中心
- 长沙中安密码检测有限公司
- 北京信息安全测评中心



2

中国商用密码市场情况

商密主要企业对比



公司名称	主要产品	产品特点	发明专利和软件著作权	营业收入	净利润	研发人员及研发费用占比	客户构成
数字认证	电子认证服务、安全集成、安全咨询和运维服务。	公司致力于保障用户信息基础设施安全可靠运行、保护用户信息化业务安全可信开展、保卫用户数字资产。	截止2019年12月31日，公司有专利12项，软件著作权140项。	2019年，公司实现营业收入7.94亿元，较上年同期增长18.90%。其中，电子认证服务收入为2.63亿元、安全集成收入为3.48亿元、安全咨询和运维服务1.84亿元。	2019年，归属于母公司所有者的净利润为9,852.60万元，较上年同期增长13.96%。	截止2019年末，研发人员774人，占比65.00%；2019年度，研发投入1.42亿元，占营业收入比例17.89%。	政府机构、金融、医疗卫生、教育交通、大型企业等。
卫士通	密码产品、网络安全产品、行业应用安全产品、安全集成与运营服务。	公司产品主要解决用户数据在网络处理与存储、网络接入、传输与交换、网络管理等过程中的信息的安全，实现通信网络和信息系统的安全和保密。	截止2019年12月31日，公司有143项发明专利，374项软件著作权。	2019年，公司实现营业收入21.04亿元，同比增长8.95%。其中，单机和系统产品收入为8.64亿；安全服务与集成收入为12.40亿。	2019年，归属于母公司所有者的净利润为1.56亿元，同比增长29.58%。	截止2019年末，研发人员853人，占比员工总人数比例为41.39%；2019年度，研发投入为2.47亿元，占营业收入比例11.73%。	政府机构、银行、国有大型企业等。
格尔软件	PKI基础设施产品、PKI安全应用产品和通用安全产品。	公司专注于信息安全行业PKI领域，主要从事以公钥基础设施PKI为核心的商用密码软件产品的研发、生产和销售及服务业务，为用户提供基于PKI的信息安全系列产品、安全服务和信息安全整体解决方案。	截止2019年12月31日，公司有41项发明专利，106项软件著作权。	2019年，公司实现营业收入3.71亿，较上年同期增长20.08%。其中，PKI基础设施产品收入为0.67亿元、PKI安全应用产品收入为1.81亿元、通用安全产品收入为1.23亿元。	2019年，归属于母公司所有者的净利润为7,007.52万元，较上年同期降低2.40%。	截止2019年末，研发人员365人，占比70.19%；2019年度，研发投入为6,108.84万元，占营业收入比例16.49%。	国家部委、地方政府部门、金融机构、军工、大中型企事业单位。

商密主要企业对比

更多资料，欢迎访问 www.wenku120.com



公司名称	主要产品	产品特点	发明专利和软件著作权	营业收入	净利润	研发人员及研发费用占比	客户构成
吉大正元	电子认证产品、信息安全服务和安全集成。	公司为用户提供第三方电子认证、系统运维与保障、技术开发、第三方安全运营、安全咨询、云安全服务等支撑，将各类信息安全软硬件产品和技术有机结合，为客户提供定制化的信息安全解决方案。	截止2019年12月6日，公司有6项发明专利，226项软件著作权。	2018年，公司实现营业收入4亿元，较上年同期降低4.28%。其中，电子认证产品收入为2.26亿元、信息安全服务收入为0.96亿元、安全集成收入为0.78亿元。	2018年，归属于母公司所有者的净利润为8,792.66万元，较上年同期增长58.09%。	截止2018年末，研发及技术人员575人，占比75.56%；2018年度，研发投入为3,192.84万元，占营业收入比例7.98%。	覆盖了政府、军队、军工、金融、能源和电信等众多行业和领域。
信安世纪	身份安全、通信安全、数据安全、移动安全、云安全和平台安全。	公司以密码技术为基础支撑，致力于解决网络环境中的身份安全、通信安全和数据安全等信息安全问题。	截止本招股说明书签署日，公司已经累计取得62项专利（其中发明专利45项）、138项软件著作权。	2019年，公司实现营业收入为3.18亿元，较上年同期增长18.01%。其中，信息安全产品收入为2.89亿元、信息安全服务收入为0.28亿元。	2019年，归属于母公司所有者的净利润为9,034.80万元，较上年同期增长15.69%。	截止2019年末，研发人员260人，占比40.75%；2019年度，研发投入4,496.88万元，占营业收入比例为14.15%。	金融、交通、人社、烟草、民航、税务、电信运营商等行业和领域。

数据来源：同行业可比公司的招股说明书、年度报告及官方网站等公开资料



应用分类

商用密码产品按功能可以划分为七类：密码算法类、数据加解密类、认证鉴别类、证书管理类、密钥管理类、密码防伪类和综合类。

1、密码算法类产品

密码算法类产品主要是指提供基础密码运算功能的产品，如密码芯片等。

•算法芯片

算法芯片以实现密码算法逻辑为主，一般不涉及密钥或敏感信息的安全存储，如椭圆曲线密码算法芯片、数字物理噪声源芯片。

•安全芯片

安全芯片在算法芯片的基础上，增加了密钥和敏感信息存储等安全功能，相当于一个“保险柜”，最重要的算法数据都存储在芯片中，加密和解密的运算是在芯片内部完成的。

类别	解释	典型产品
密码算法类	构成密码应用基础的能提供密码运算功能的产品	密码算法实现软件、密码算法芯片等产品
数据加密类	提供数据加密解密功能的产品	加密机、加密卡、智能密码钥匙等产品
证书管理类	提供身份认证、密码鉴别功能的产品	动态口令系统、身份认证系统
密钥管理类	提供密钥的产生、分发、更新、归档和恢复等功能的产品	密钥管理系统等产品
密码防伪类	提供密钥防伪验证功能的产品	电子印章系统、支付密码器、数字水印等产品
综合类	提供上述两种或两种以上功能的产品	电子商务安全平台等产品

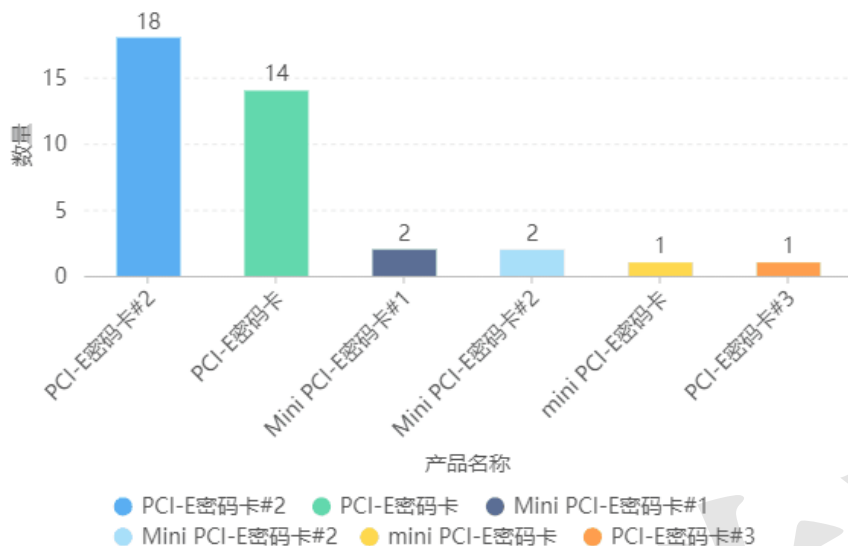
类别	解释	典型产品
密码软件类	提供纯软件形态出现的密码产品	信息加密软件、密码算法实现软件等产品
密码芯片类	以集成电路芯片形态出现的密码产品	密码算法芯片、密码 SOC 芯片等产品
密码模块类	以多芯片组装的背板形态出现，具备专用密码功能，但本身不能完成完整的密码功能的产品	加解密模块、安全控制模块等产品
密码板卡类	以板卡形态出现，具备完整密码功能的产品	USB 密码钥匙、PCI 密码卡等产品
密码整机类	以整机形态出现，具备完整密码功能的产品	VPN、网络密码机、服务器密码机、签名验证服务器等产品
密码系统类	以系统形态出现，由密码功能支撑的产品	安全认证系统、私钥管理系统等产品

2、数据加解密类产品主要是指提供数据加解密功能的产品，如服务器密码机、VPN设备、加密硬盘等。

3、认证鉴别类产品主要是指提供身份鉴别等功能的产品，如认证网关、动态口令系统、签名验签服务器等。

密码卡分析

加密卡数量



- 1、《密码设备应用接口规范》(GM/T0018-2012)
- 2、《SM2椭圆曲线公钥密码算法》(GM/T0003-2012)
- 3、《SM3密码杂凑算法》(GM/T0004-2012)
- 4、《SM4分组密码算法》(GM/T0002-2012)
- 5、《SM9标识密码算法》(GM/T0044-2016)
- 6、《随机性检测规范》(GM/T0005-2012)
- 7、《PCI密码卡技术规范
- 8、《密码应用标识规范》(GM/T 0006-2012)
- 9、《SM2密码算法使用规范》(GM/T 0009-2012)

主要厂商

See
Data



作为国内首款三级密码模块，可以为您提供符合等级保护三级、等级保护四级的密码安全支撑能力。具备SR-IOV虚拟化功能，为云中加密场景提供更多选择。



采用自主知识产权的嵌入式文件系统，提供目录及文件等管理服务，支持多卡并行多进程、多线程调用。



PCI-E高速密码卡是数盾科技利用多芯片并行技术独立自研的基础高速密码设备，40G高性能网络加密吞吐，GD01组密钥管理技术。



密码卡采用了国产的低功耗高性能的主处理器，对称、非对称运算均由专用加速芯片实现，对称运算性能达到或超过国内外同行业主流水平。

1、**全面国产**。全面国产是指包括硬件研发、芯片研发制造、软件编程、制造、销售等等全都是国产自主可控。一是信息安全行业趋势如此，二是出于现实的保密需要。

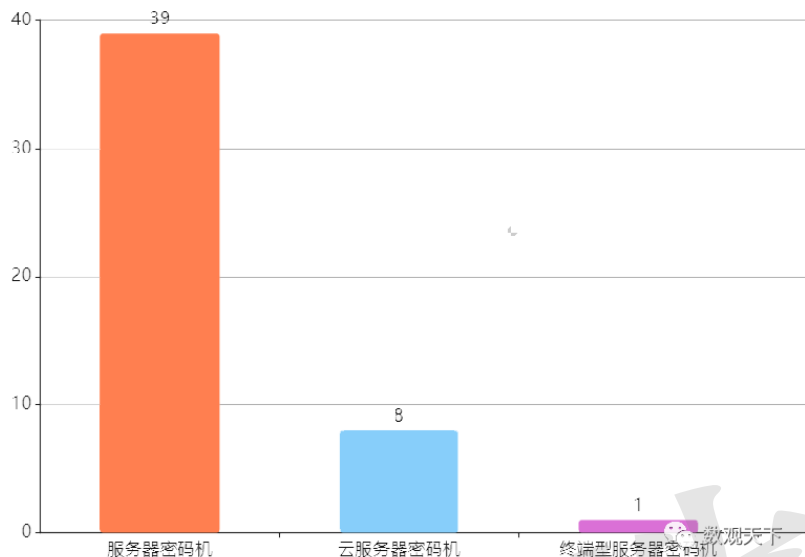
2、**高性能**。只有更高的性能才能做到更好的适用性。因为各个行业的硬件都在更新换代、尤其是信息技术行业，硬件更新较快，其他硬件的性能提升必然要求密码卡的性能也随之提升，另外有些应用对性能需求远大于现在密码卡所能达到的水平，进而无法适用现在的密码卡。所以密码卡只有性能获得成倍上升才可能得到更广泛的应用。

3、**小型化**。现在很多设备的设计和制造越来越注重移动、便捷、便携。这也意味着密码卡也要更加的小巧才行。而硬件的小型化还意味着散热、功率、结构等全面改变。

4、**智能化**。未来的硬件设备都将会有一定的智能化需求，密码卡也不例外。这意味着更复杂的软件设计研发和更多的指令集和信息库。只有更加智能，才能满足更多的需求。

服务器密码机产品分析

服务器密码机数量



- 1、GM/T 0030-2014 《服务器密码机技术规范》
- 2、GM/T0059-2018 《服务器密码机检测规范》
- 3、符合《商用密码产品随机数检测要求》

主要厂商

See
Data



DONJIN

提供多种开发接口，简单、方便的与应用系统集成；支持密码机集群，适应云计算的大趋势；提供安全、方便、易用的维护监控系统，大大降低设备的维护成本

TASS

江南天安

密码芯片、随机数发生器、电源等主要器件采用多路硬件冗余设计，保障系

统的稳定性和连续性

SJS

中安网脉
SINOINFOSEC

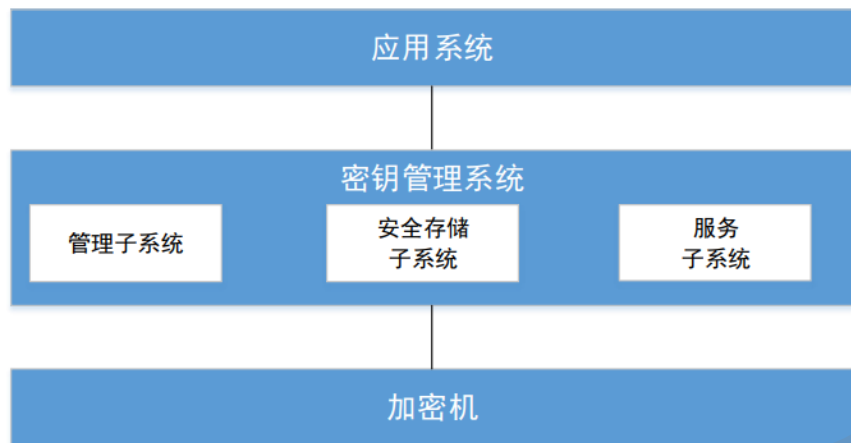
SJJ1524服务器密码机是中安网脉（北京）技术股份有限公司自主研发的一款应用层密码设备，为业务应用系统提供数据加解密、签名验证、杂凑等密码运算服务

江南信安
JIANG NAN INFORMATION SECURITY

可以提供多种国产密码算法（SM1、SM2、SM3、SM4），并能够保证密钥和密码算法安全性，具有很高的安全性和实用价值。符合GM/T 0018-2012《密码设备应用接口规范》，可以安全、灵活、方便的集成到各类安全应用系统中。

- 1、**多加密卡使用：**在密码机中插入2-3个加密卡，可以多个卡之间协同高效并行工作，提高密码机的加解密的服务速度。
- 2、**多网卡使用：**可以考虑在服务器密码机中插入2块或3块网卡，实现系统冗余和负载均衡。
- 3、**完善的安全管理机制：**为了使服务器密码机更加稳定、安全的运行，必须提供完善的日志和审计功能，用来记录有关性能、入侵和攻击等异常情况，并且能够分析和报警
- 4、**实现新的加解密算法：**现今所支持的密码学算法都是为人所共知的，而随着计算机性能的提高，其中的许多算法的破译已变得相当容易，为了保证用户的安全应用系统的安全性，应不断对密码机支持的算法进行升级和更新。

密钥管理系统产品分析



- 1、GM/T 0034-2014《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》
- 2、GM/T 0005《随机性检测规范》
- 3、GM/T 0028《密码模块安全技术要求》
- 4、GM/T 0051《密码设备管理 对称密钥管理技术规范》

主要厂商



信安世纪密钥管理系统使用不同的管理方式、遵照不同的技术规范、支持不同的密钥类型和算法来满足安全市场日益多样化的需求，信安世纪密钥管理系统将全面服务于客户需要加密的任何场合，对数据、视频、信息等所有需要保护的内容完成密钥分发、加解密等全生命周期管理。



江南科友将密钥管理中的要素抽象为模板，为客户提供一个密钥管理设计和实施的平台，使客户可以根据自身业务密钥管理的需求灵活设计符合业务系统需要的密钥管理方案。



密钥管理系统由对称密钥和非对称密钥管理模块组成，同时采用配置化管理，满足用户多应用、多业务密钥管理需求。

- 1、**云计算环境**：云服务中的数据归云用户所有，但是数据物理驻留的存储资源受云供应商的控制。另外 KMS 一般也运行在云供应商提供的计算资源上。这样，能否从那些加密操作上寻求到必要的安全保证是云环境下的密钥管理用户不得不面对的问题。
- 2、**密钥数量大**：通过公开网络将大量敏感信息（密钥信息）从客户手中传递到云服务提供商的过程中会存在诸多安全风险，例如：窃听、钓鱼，因此要设计分布式密钥分发机制，
- 3、**代理重加密技术**：使用代理重加密技术，未加密的对称密钥绝不会暴露在服务端。即使被攻破，黑客也只能得到重新加密的密钥，并且对文件的访问任然受到保护。

身份认证系统分析



- 1、GM/T 0021 《动态口令密码应用技术规范》
- 2、GM/T 0028 《密码模块安全技术要求》
- 3、GM/T 0027 《智能密码钥匙技术规范》

主要厂商



公司 PKI 产品的市场竞争优势明显，并获得了业内的高度认可，已成为信息安全行业中 PKI 领域的优势企业之一



专注于数字安全的两个核心领域：安全和认证。将安全软件嵌入设备和物体中，跨不同网络保护和加密数据



统一认证管理系统以用户身份管理为核心，加强管理B/S、C/S、移动APP等结构的多应用的安全访问机制，集身份管理、身份认证、授权管理、应用资源访问控制及其安全审计于一体，构建多信息资源的应用整合、集约管理和安全防护的安全基础服务平台。



吉大正元
信息技术股份有限公司

吉大正元在PKI电子证书认证系统领域处于领先地位。IDC数据报告也连续多年确认了吉大正元在国内信息安全应用领域软件市场占有率第一的地位。

1、**统一密码服务平台**：实现统一的密码设备资源管理、弹性调度，以及密钥管理、密码计算能力的服务化，为上层业务应用提供安全高效的密码服务支撑。

2、**云PKI**：适应移动互联、云计算环境的下一代 PKI/CA 服务产品，可以应对大规模多样化的移动端、云平台带来的安全挑战。

3、**零信任**：包括云身份服务系统、零信任网关、安全策略管理中心。和传统安全产品的区别在于采用云服务架构设计，通过实现先认证后访问、持续信任评估、动态访问控制等功能，帮助企业在新 IT 环境下构建零信任安全体系。

4、**区块链技术**：拟研发自主可控的面向联盟链的区块链技术平台，以打造区块链密码支撑环境、区块链应用开发和实施体系。

物联网安全产品分析



- 1、GM/T 0002-2012 SM4分组密码算法
- 2、GM/T 0003-2012 SM2椭圆曲线公钥密码算法
- 3、GM/T 0004-2012 SM3密码杂凑算法
- 4、GM/T 0005-2012 随机性检测规范
- 5、GM/T 0009-2012 SM2密码算法使用规范
- 6、GM/T 0028-2014 《密码模块安全技术要求》
- 7、GM/T 0039-2015 《密码模块安全检测要求》

主要厂商



中宇万通 ZHYU TECHNOLOGIES 公司保持较高的核心技术研发能力和研发创新力度, 物联网安全、云安全领域率先投入研发, 推出视频安全网关、签名服务器、智能应用网关、行为管理系统等产品



天融信 TOPSEC 天融信基于物联网国密安全标识系统(TID)的安全解决方案可以提供物联网可信密码标识技术从而保障物联网设备身份唯一性。



海泰方圆 Haitai 海泰方圆拥有物联网终端密码模块系列、移动智能终端密码模块(软)、智能密码钥匙、物联网云密码服务平台等各类产品, 能够提供物联网融合场景商用密码应用体系化解决方案



ANYDEF 安智融合 现拥有国内领先的基于生物识别的智能身份识别、统一密码服务、物联网安全管理, 信息安全集成等四大产品线

- 1、**物联网感控设备**: 攻击者可利用鉴别机制弱点恶意部署同型号或克隆一个相似设备, 接入系统进行攻击。
- 2、**安全网关**: 由于物联网终端可能采集处理大量敏感数据, 若安全网关对上述数据转发未作加密, 则易发生数据窃取等问题。
- 3、**无线安全**: 物联网中节点数量庞大且数据传输采用无线射频信号进行传输, 存在攻击者可通过发射干扰信号造成通信中断, 或信号传输过程中劫持、窃听、篡改数据等风险
- 4、**数据交换**: 传输层面临异构网络跨网认证等安全问题, 此外, 物联网上传输的数据包未加密和签名, 易发生被窃听、篡改、伪造以及发送者抵赖等问题
- 5、**业务平台**: 由于接入设备类型繁多、能力参差不齐, 存在身份仿冒、非授权访问等安全风险。

商用密码媒体公众号



主要媒体

See
Data



国家密码管理局公众服务号，是发布政务信息、提供在线服务、宣传密码政策法规、普及密码知识、促进密码应用的重要渠道。



由中华人民共和国信息产业部主管，中国电子科技集团第三十研究所主办，中国信息安全测评认证中心、国家保密技术研究所和中国计算机学会信息保密专业委员会协办。是经国家新闻出版署批准出版的我国第一家、面向信息安全与通信保密行业、大型综合指导性技术月刊。



《中国信息安全》杂志，介绍国内外最新网络安全动态，深度解读网络安全事件。



密码基础知识、最新密码技术、密码解决方案、密码应用场景解析、商用密码产品检测、商用密码应用安全性评估的相关标准解读、案例分析与注意事项等相关知识与资讯共享平台。



纵观密码安全行业全局，第一时间更新国内外密码安全大事件。关注所有密码人关心的一切，分析国内外密码安全行业发展动向。



商密君是全国密码行业头部公众号，旨在宣传推广《密码法》，普及商用密码知识，解读密码政策，分享商用密码行业的最新动态，为密码产业产学研用做好宣传服务，连接密码全行业精英，推动密码技术在数字经济各行业的应用和创新。



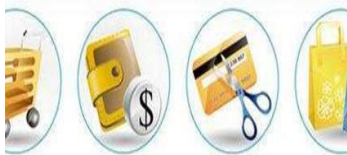
解读密码法律法规、普及密码行业知识、提供密码改造咨询服务，致力于成为“密码改造创新服务中心”



产品主要领域

金融领域

消费金融



使用金融IC卡、动态令牌、智能密码钥匙等实现对客户身份、服务器等进行认证；

使用密码技术，实现对系统存储的用户口令、用户隐私信息、重要交易数据等的加密保护

电子政务领域

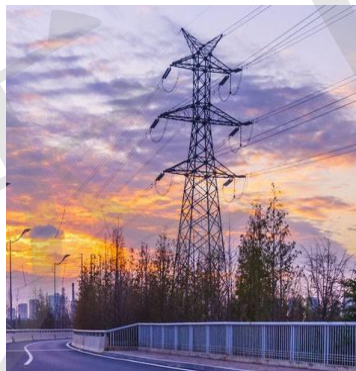


利用密码技术增加安全防护，确保网络数据的安全传输。

基于PKI技术的电子认证，对网络上传输的数据进行加密、解密。

采用SM9算法和数字签名实现身份认证和邮件内容加密。

电力领域

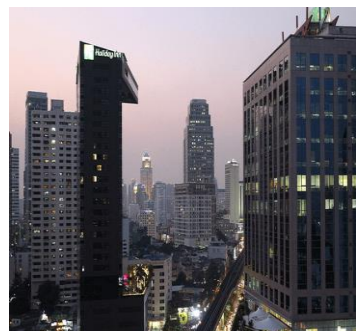


发电环节，基于商用密码的电子认证体系，实现调控指令的可靠执行。

输电环节，采用数据加密、身份鉴别方法，保障输电环节安全。

变电环节，通过部署纵向加密装置，保证业务传输数据安全及身份认证。

信息网络领域



密码安全协议包括：优先局域网安全TLSec技术、无线局域网安全WAPI技术、IP安全可信TISec技术、射频识别RFID空中接口安全TRAIS技术等。

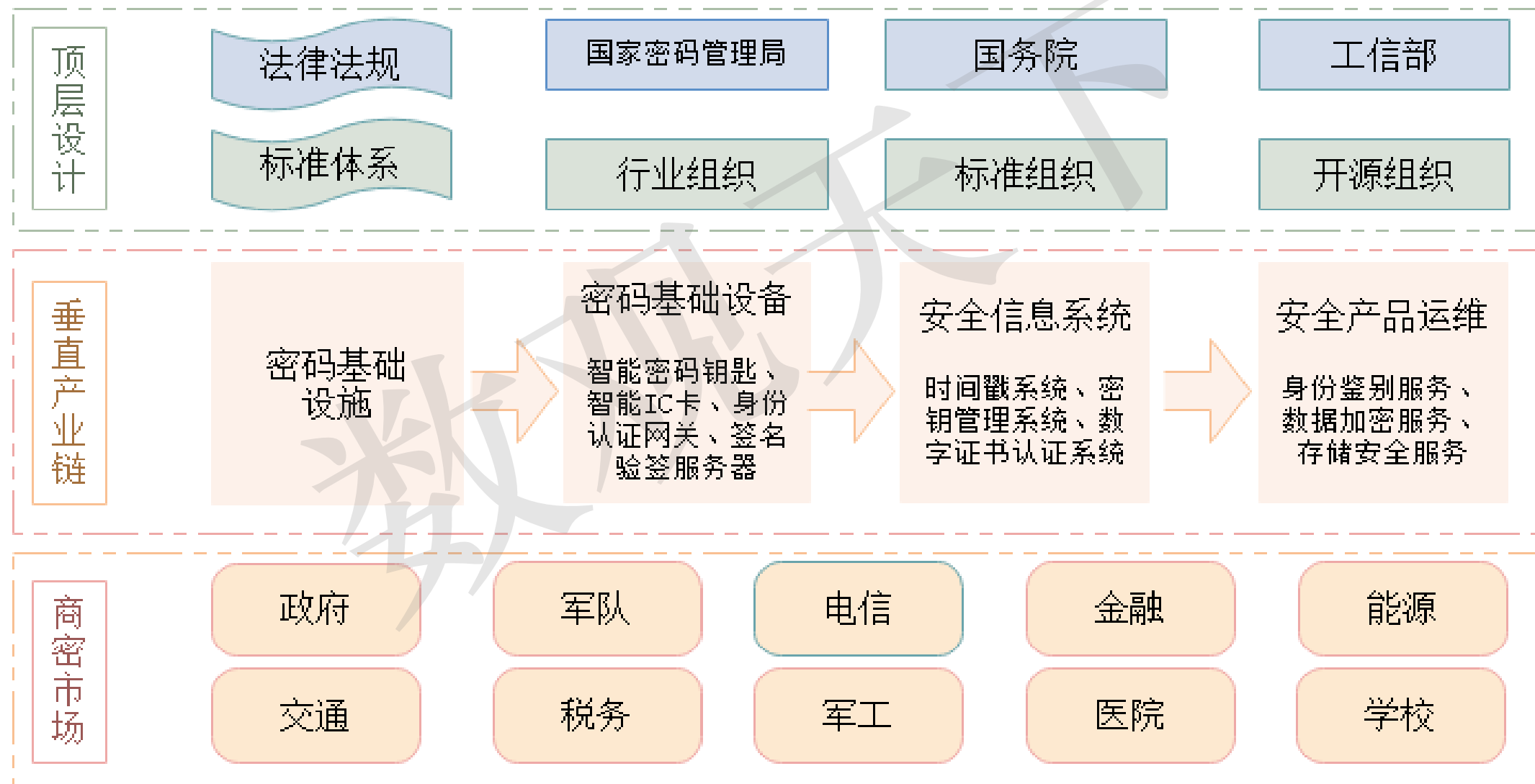


3

中国商用密码产业链分析



产业链分析



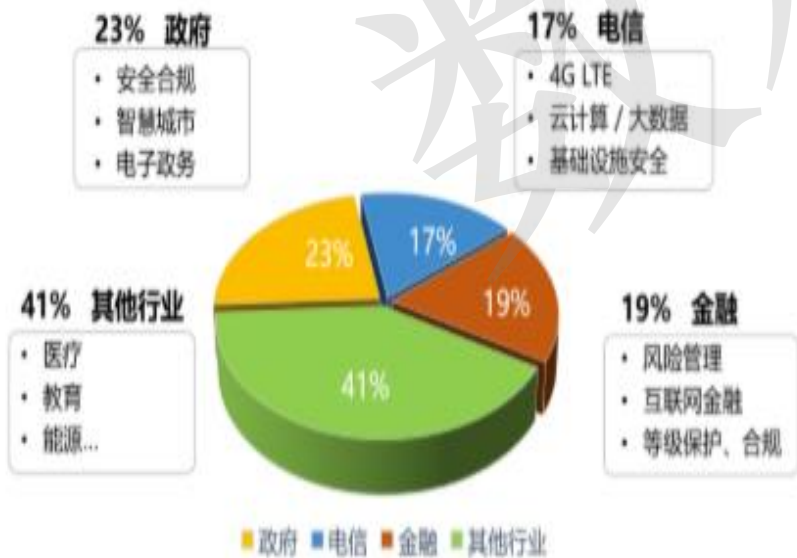


产业链分析

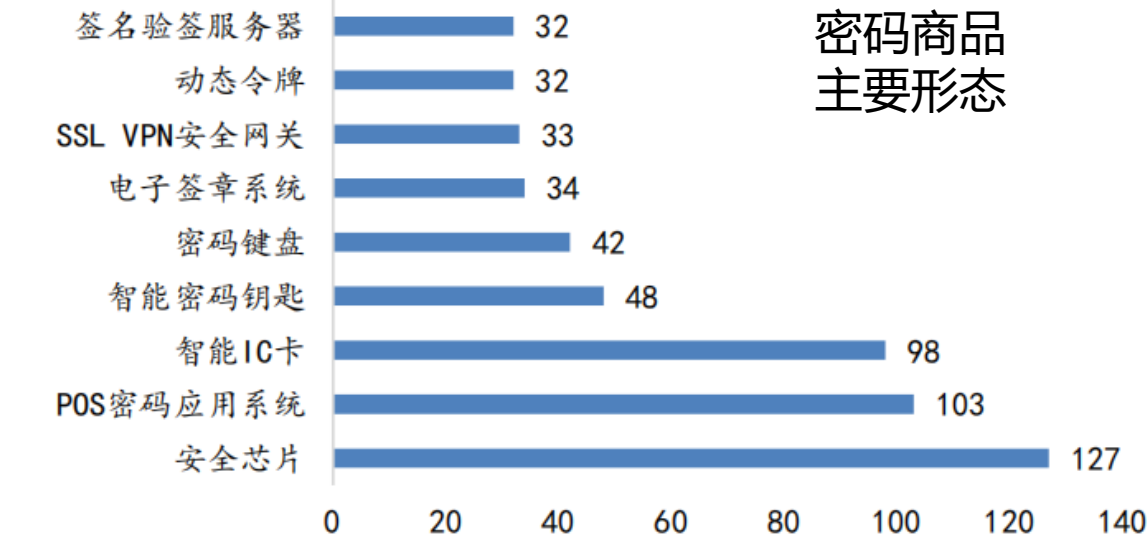
产业链内各企业也可能同时处于不同的位置。如成都卫士通，既处于行业最上游，可以为下游企业提供密码机、加密卡等产品，又是电子认证产品生产商，位于行业中游，可以提供电子认证系统及服务。产业链上游主要为密码设备供应商，处于电子元器件、IT设备及软件开发工具等软硬件生产制造行业。供应的产品如加密机、密码卡、USB KEY 等。受我国密码政策的影响，对行业上游企业实施市场准入制度，上游企业均为内资企业，数量众多，而且随着国产自主可替代计划的推进，电子元器件、集成电路、安全芯片趋于国产化，对国外提供商的依赖有所降低。总体来看，上游原材料供给稳定，产品价格和质量较稳定，上游行业的波动对公司所处行业的影响较小。

下游为对信息安全具有较高要求的应用行业，主要为政府、军队、军工、央企、科研院所、金融、能源等行业，以及云计算、物联网等领域的各级用户。下游行业总体的信息化进程仍处于快速发展阶段，信息化发展促进了信息安全及密码产品、集成及服务需求持续增长。

客户分布



密码商品主要形态





产业链分析

对本案所在的商用密码产业链，其上中下游，依次为：

上游——密码/安全芯片、印刷电路板、服务器等IT设备及软件开发工具，代表公司包括浪潮信息（毛利率11.88%）、深南电路（毛利率26.53%）、生益科技（毛利率26.65%）。

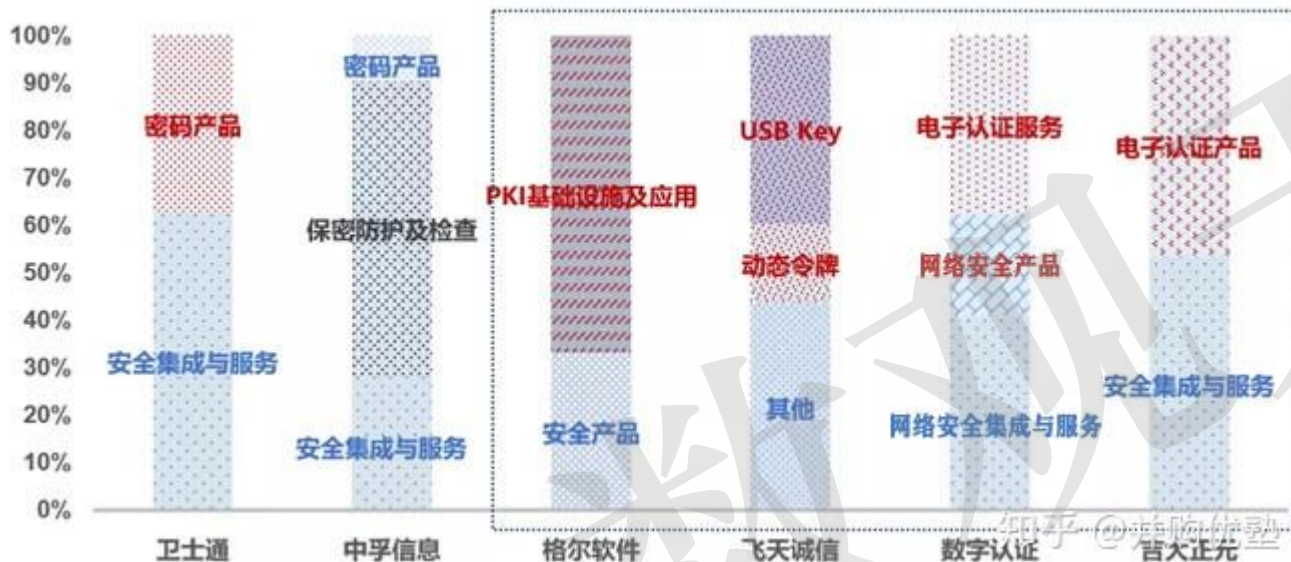
中游——以密码技术为核心的产品、服务提供商，产品包括智能IC卡、智能密码钥匙（USB Key）、密码机、电子签章、数字证书认证系统等。代表公司包括卫士通（毛利率32.54%）、飞天诚信（38.37%）、中孚信息（69.87%）、格尔软件（58.56%）、数字认证（60.27%）、启明星辰（65.79%）、奇安信（56.72%）、深信服（72.19%），以及综合网安厂商，部分产品涉及密码技术，如启明星辰（65.79%）、奇安信（56.72%）、深信服（72.19%），以及硬盘等电子产品巨头Western Digital、Samsung Electronics。（对启明星辰、深信服、奇安信，我们在科技版报告库中，都做过研究，此处不详述）

下游——客户主要是机关、军工、银行、证券，以及大型企业集团。



产业链分析

我们选取产品以密码技术为核心业务的几家龙头，做对比：卫士通VS飞天诚信VS格尔软件VS吉大正元VS数字认证进行对比，梳理商用密码领域的核心逻辑。从2020年上半年收入体量来看：卫士通（4.33亿）>飞天诚信（3.52亿）>数字认证（2亿）>吉大正元（1.86亿）>中孚信息（1.76亿）>格尔软件（1.12亿）。



从收入结构来看：

卫士通——37.06%来自单机和系统产品（各类商用密码产品），62.94%来自安全集成与服务（以密码产品为基础的集成业务）。

格尔软件——48.79%来自PKI安全应用产品（安全认证网关、电子签章系统等），18.04%来自PKI基础设施产品（数字认证系统、密钥管理系统等），33.18%来自通用安全产品。

飞天诚信——39.55%来自USB Key，16.79%来自动态令牌，14.86%来自智能终端（云音箱、扫码盒子等）。

数字认证——37.37%来自电子认证服务，32.87%来自网络安全服务，21.62%来自网络安全产品，8.14%来自网络安全集成。

吉大正元——23.96%来自信息安全服务（包括认证服务和咨询服务）、46.6%来自电子认证产品、29.44%来自安全集成。

中孚信息——48.03%来自保密防护产品、8.99%来自保密检查产品、28.47%来自信息安全服务（涉密信息系统集成），商用密码产品（USB Key等）仅占比3.76%。

我们以2020年三季报数据为基础，分别对比一下几家的增长情况

	营业收入	归母净利润	销售毛利率	销售净利率	营业收入增速	净利润增速
卫士通	9.80	-0.94	35.73	-9.91	-6.09	-47.52
飞天诚信	5.79	0.34	41.87	6.07	-2.66	14.56
数字认证	4.07	0.17	59.06	4.29	0.74	-60.10
中孚信息	3.79	0.20	67.75	5.22	25.27	44.16
吉大正元	2.83	0.28	62.33	11.57	-2.75	3.78
格尔软件	1.76	-0.34	54.31	-19.24	16.07	-512.42

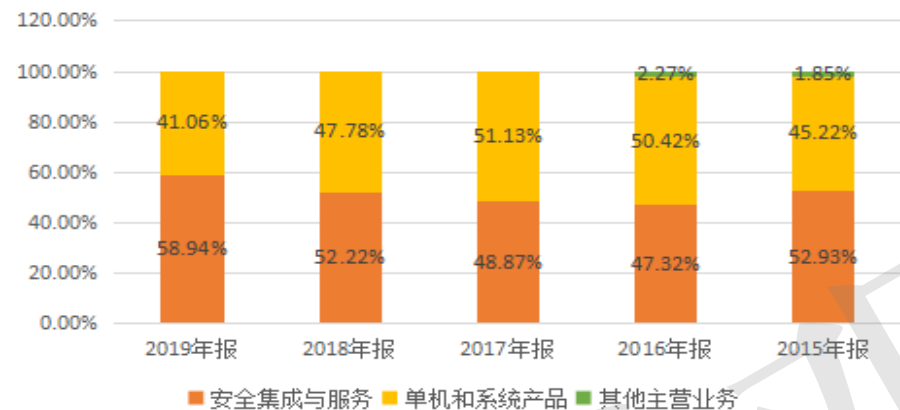
2020年三季报数据（单位：人民币/亿、%）

数据来源：塔坚研究



上市公司经营状况|卫士通

主营业务收入构成



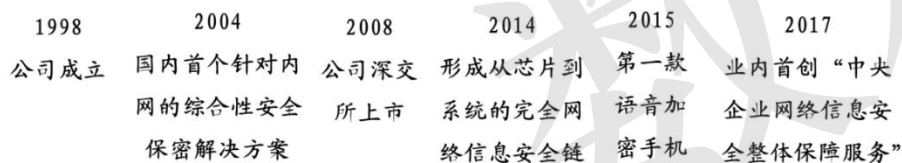
1. 基本介绍： 公司成立于1998年，是国内知名密码产品、网络安全产品、互联网安全运营、行业安全解决方案综合提供商，首批商密产品研发、生产、销售资质单位，首批涉密信息系统集成甲级资质单位，国内专业从事网络信息安全的上市公司，专注网络信息安全，致力打造从芯片到系统的全生命周期安全解决方案，为党政军用户、企业级用户和消费者提供专业自主的网络信息安全解决方案、产品和服务。公司自成立以来一直致力于信息安全领域的技术研究及产品开发，公司从密码技术应用持续拓展，已形成密码产品、信息安全产品、安全信息系统三大信息安全产品体系，同时，基于ISSE体系框架，为党政、央企、能源、金融等用户提供以“安全咨询、风险评估、运维与应急响应”为主要内容的信息系统全生命周期的安全集成与运营服务。

2. 主营业务：

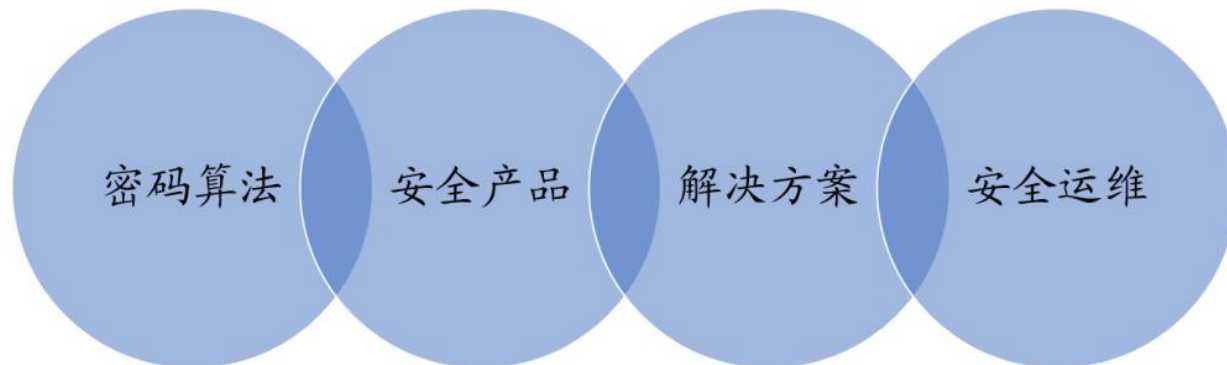
- a. 安全集成与服务：包括密码产品、网络安全、数据安全、端点安全、云安全、移动安全等；
- b. 单机及系统产品：主要为客户解决安全相关的解决方案。

3. 主要客户： 政府、公检法、金融、电子政务、能源等。

4. 财务情况： 2019年营业收入21.04亿元，同比增长8.95%，净利润1.56亿元，同比增长29.58%。



具备安全产品、解决方案、安全运维一体化密码服务能力





上市公司经营状况|数字认证

主营业务收入构成



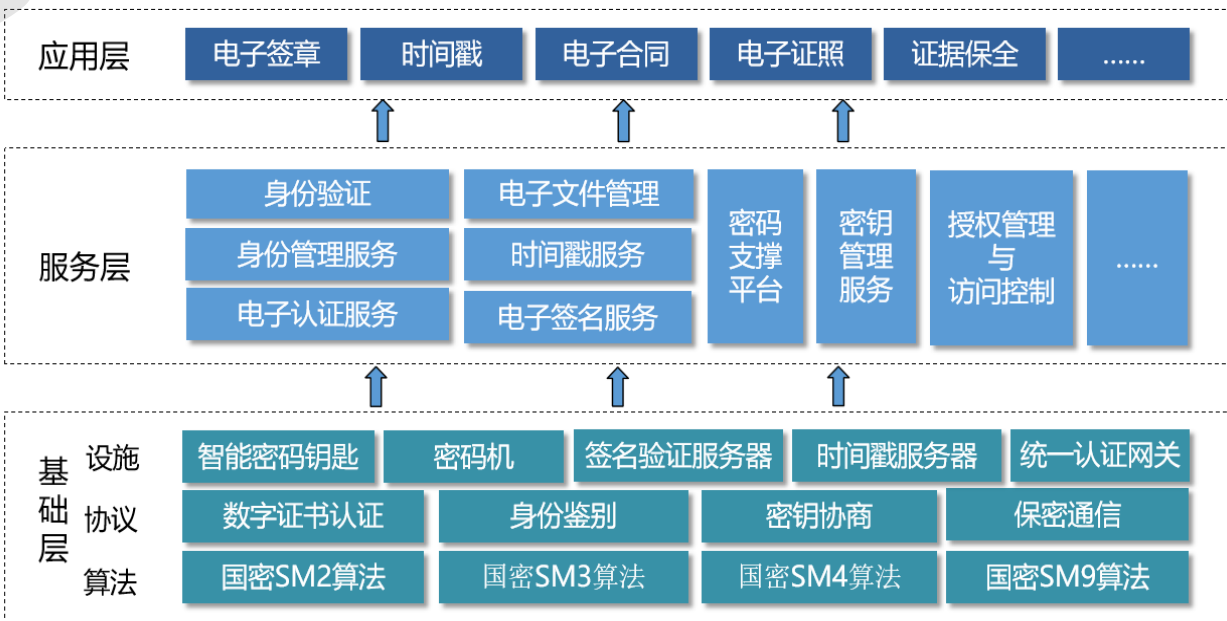
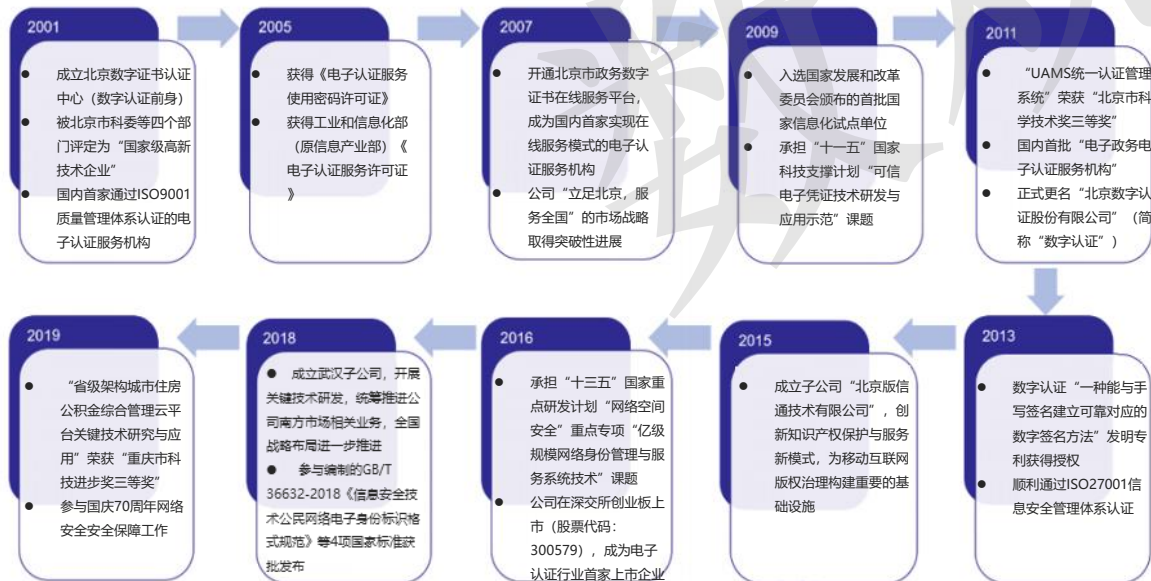
1. 基本介绍：北京数字认证股份有限公司（简称：数字认证）是领先的网络安全解决方案提供商，坚持“共建可信任的数字世界”的企业愿景、以“提供高品质的网络安全服务，帮助用户构建安全可信的网络空间”作为公司使命，始终致力于保障用户信息基础设施安全可靠运行、保护用户信息化业务安全可信开展、保卫用户数字资产。公司面向全国客户提供电子认证服务、安全集成、安全咨询与运维服务，并在政务、金融、医疗卫生、教育、交通等领域建立领先优势。

2. 主营业务：

- a. 电子认证服务：主要包括数字证书和电子签名两类服务。
- b. 安全集成业务：为客户提供适合其信息系统特点的网络安全保障解决方案。
- c. 安全咨询及运维服务：风险评估、合规性咨询、代码审计、脆弱性检查、渗透测试、安全巡检等

3. 主要客户：覆盖政府机构、金融、医疗卫生、教育、交通、大型企业等。

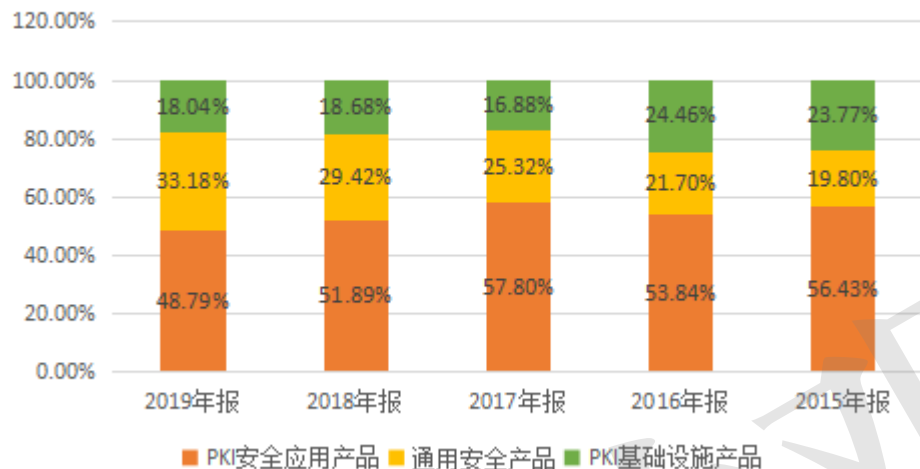
4. 财务情况：2019年营业收入7.94亿元，同比增长18.90%，净利润9852.6万元，同比增长13.96%。





上市公司经营状况|格尔软件

主营业务收入构成



PKI基础设施产品



数字证书认证系统



身份认证系统



密钥管理系统

PKI安全应用产品



安全认证网关



安全电子邮件系统



签名验证服务系统



打印管控系统



可信边界安全网关



安全即时通系统



局域网接入认证系统



移动介质管理系统



无线安全网关



网络保险箱



移动安全管理平台



云安全服务平台系统



电子签章系统



终端保密系统



云安全服务平台系统

通用安全产品



网络审计系统



信息安全系统集成

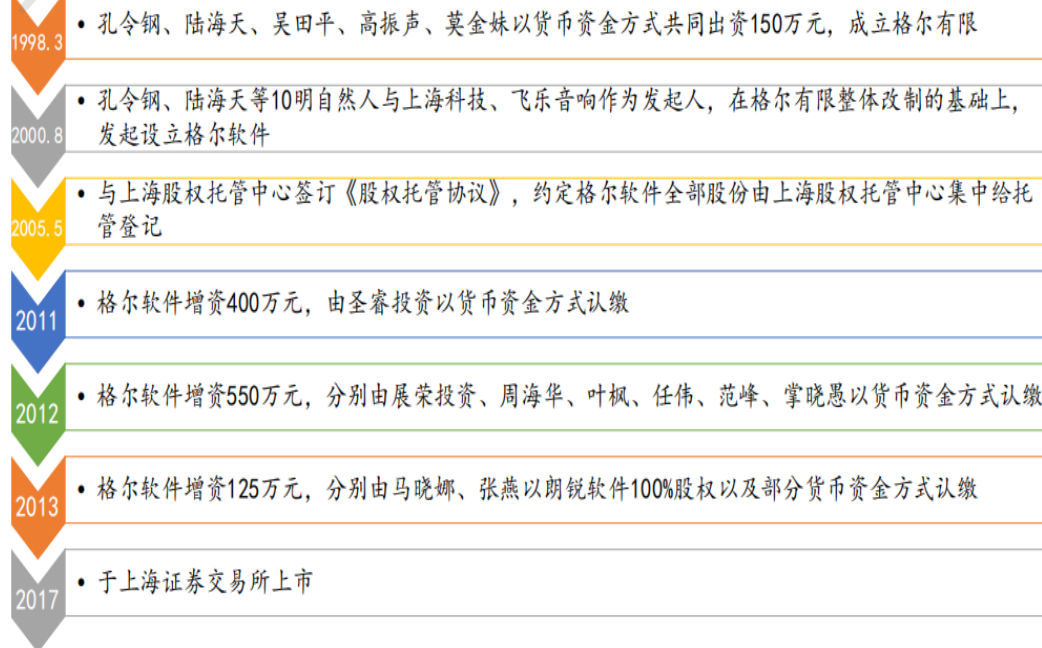
1. 基本介绍： 公司成立于 1998 年 3 月，公司于 2017 年 4 月在上交所挂牌，公司自成立以来就专注于以 PKI 为核心的商用密码产品等信息安全产品与系统的研发、生产和销售，为用户提供基于PKI的信息安全系列产品、安全服务和信息安全整体解决方案。公司先后被评为国家高新技术企业、国家火炬计划重点高新技术企业。公司是信息安全行业中 PKI 产品市场的先行者和优势企业，凭借业已形成的综合竞争优势，公司研发、生产、销售的PKI基础设施与PKI安全应用产品在前述市场具有领先优势。

2. 主营业务：

- PKI 基础设施产品；
- PKI 安全应用产品；
- 通用安全产品

3. 主要客户： 国家部委、地方政府部门、公安、军工、金融机构、CA公司、大中型企事业单位。

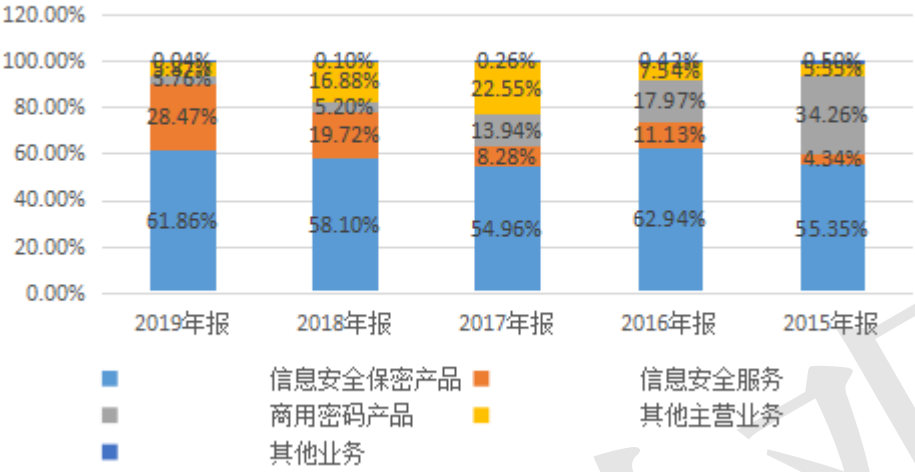
4. 财务情况： 2019年营业收入3.71亿元，同比增长20.08%，净利润7007.52万元，同比增长-2.40%。





上市公司经营状况|中孚信息

主营业务收入构成

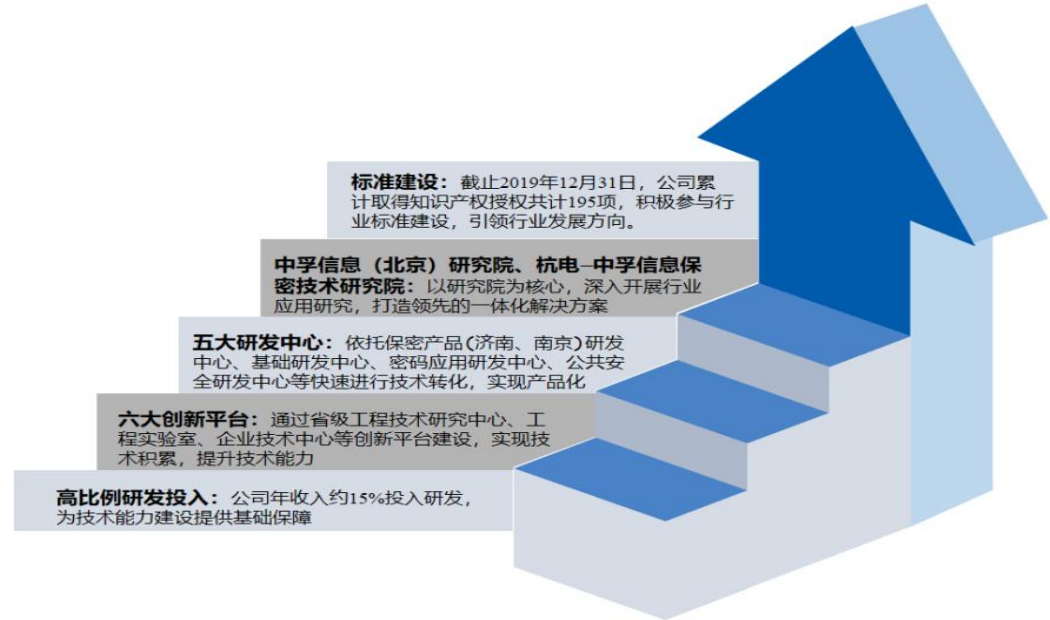
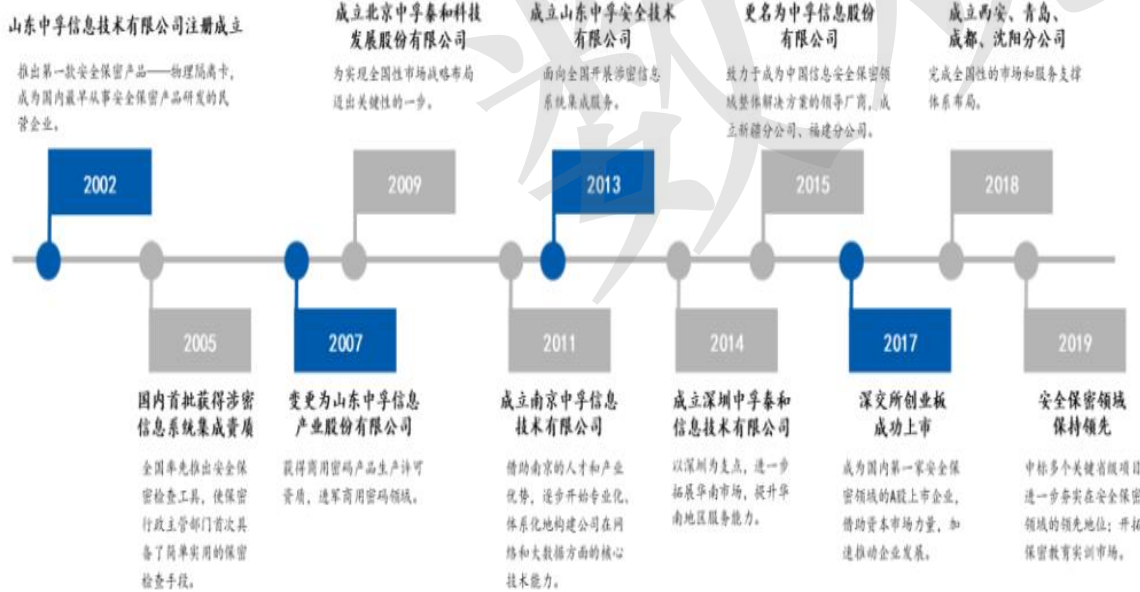


1. 基本介绍： 中孚信息成立于 2002 年，重点围绕安全保密、密码应用、公共安全等业务领域，形成了全系列的安全产品和面向分级保护、等级保护等党政内网的产品和行业应用解决方案。公司成立初期，凭借隔离卡、检查工具、清除工具等多个产品确立了市场先发优势，在保密领域积累了大量客户；2005 年，公司在国内率先推出具有深度数据恢复技术的安全保密检查工具，并在全国 20 多个省份的保密系统进行推广、配备。目前，公司已设北京、南京、山东、深圳四个全资子公司，成都、西安、青岛等 9 个分公司，完成全国性的市场和服务支撑体系布局。

- 2. 主营业务：**
- a. 安全保密：包括保密防护产品、保密监管产品、保密检查产品、整体解决方案；
 - b. 密码应用：包括客户端产品、服务端产品、系统类产品、解决方案
 - c. 信息安全服务：包括涉密系统工程的规划、设计、开发、实施、服务及保障等
 - d. 公共安全解决方案：警情大数据解决方案、大数据情报可视化解决方案、关系图谱研判解决方案、协同作战指挥解决方案等

3. 主要客户： 各级政府、医疗、金融、保险、大型企事业单位等。

4. 财务情况： 2019年营业收入6.03亿元，同比增长69.32%，净利润1.25亿元，同比增长194.34%。





三未信安

主要业务/产品：包括服务器密码机、金融数据密码机、密码卡、安全认证网关等硬件产品，以及身份认证系统、密钥管理系统、数字版权管理系统等软件系统等。

公司全称：三未信安科技股份有限公司

法定代表人：张岳公

成立日期：2008-08-18

上市情况：2020年10月21日申报 科创板

公司介绍：三未信安专注于基于密码技术的产品和解决方案的研究开发、销售与服务，是国内主要的密码基础设施供应商。公司在高性能密码实现、密码模块安全、密码资源虚拟化等关键技术领域取得了一系列突破和创新性成果，推出了适用于各种应用场景的商用密码产品和密码解决方案，广泛应用于金融、证券、电力、电信、石油、交通等行业，以及海关、税务、水利、公安、医保、国家政务网等政府部门。三未信安深耕密码技术，创新践行数据安全，在商用密码领域拥有较高的市场地位和良好的口碑。

信安世纪

主要业务/产品：证书认证系统、应用安全网关、签名验签服务器、移动安全认证系统、云密码服务平台、全密码安全服务平台。

公司全称：北京信安世纪科技股份有限公司

法定代表人：马现通

成立日期：2001-08

上市情况：2020年12月11日申报 科创板

公司介绍：信安世纪是国内较早从事基于密码技术研发、生产的专业信息安全厂商之一，一直以来致力于传统互联网络、机构内部网络和移动网络在通讯传输、交易过程和网络资源保护等领域的安全实现。已成功为金融、社保、税务、海关、烟草、交通等行业提供领先的信息安全产品和解决方案，并在上千种关键信息系统中得到成功应用，是国内领先的信息安全品牌。信安世纪主持或参与了多项相关国家标准制定，承担了多项国家科研项目开发研制工作，取得了近百项技术专利。

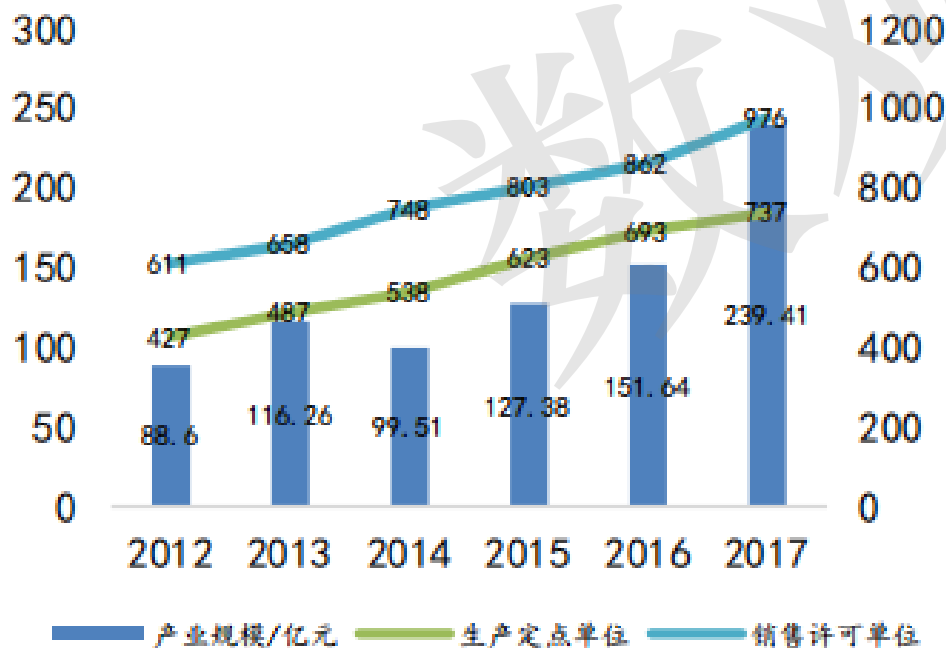
部分明星企业：商用密码领域企业国盾量子、江南天安、江南信安、苏州国芯、炼石网络、数盾科技、中创量子等均获得较大规模的投资，其中江南信安、炼石网络、数盾科技、中创量子于2020年获得投资，随着《密码法》的颁布实施，使密码市场具有巨大潜力，将会越来越多的获得投资人的青睐。



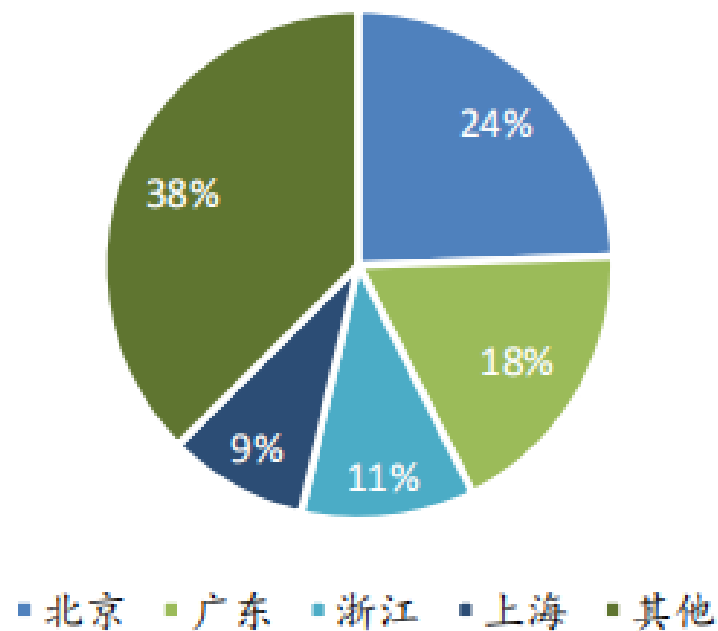
发展趋势|发展现状

随着商用密码技术不断创新，我国商用密码产业蓬勃发展。根据统计，2019年，全球商用密码市场规模达到了25041.5百万美元，预计2026年将达到86406.3百万美元，年复合增长率（CAGR）为18.79%。预计该行业将继续以创新为主导，频繁的吸收和战略联盟将成为参与者增加行业存在感的关键战略。市场处于成熟期，集中度明显。同时，优化产品结构，进一步发展增值能力，实现利润最大化。制造商可以利用这种情况，加强他们的生产单位和供应链，以避免生产周转时间（TAT）和供应交货期的任何延误。

国内商用密码产业规模及企业数量



商用密码产业区域分布





密码是保障网络与信息安全的核心技术和基础支撑，密码算法和密码产品的自主可控是确保我国信息安全的重中之重。国密算法具备自主知识产权，实现密码产品自主可控软硬件全国产化替换，是保障网络安全的重要趋势。以商用密码算法为例，我国自主设计的 SM 系列算法经过了多轮安全性分析评估，在设计、实现方面均有各自特点和优势，有力地支撑了商用密码产业化、规模化发展，得到了广泛的认可和应用。

国产替代成趋势

《密码法》对商用密码落实“放管服”改革要求，进一步削减行政许可数量，放宽市场准入。由商用密码管理条例规定的全环节严格管理调整为重点把控产品销售、服务提供、使用、进出口等关键环节，管理方式上由重事前审批更多地转为事中事后监管，重视发挥标准化和检测认证的支撑作用。“放管服”改革将极大拓宽商用密码市场规模。整个密码产业面临一个大发展的机遇，面临一个蓝海空间。这些空间以前是可望而不可即的。

密码法出台市场迎来春天

泛在化应用是密码保障的特点，密码技术正在以前所未有的广度和深度与信息技术相互促进、融合发展，为网络空间的云计算、大数据、物联网等应用保驾护航。密码服务广泛覆盖政府、企业、组织和民众，密码技术不断地向低成本、易使用逼近，密码服务已逐步成为全民服务。集密码算法、密码技术、密码产品、密码服务一体化服务化厂商将有望脱颖而出。

呈泛在化服务化趋势

商用密码产业目前产品类别较多，行业较为分散，而预计该行业将继续以创新为主导，频繁的收购和战略联盟将成为参与者增加行业存在感的关键战略。同时，资本对头部企业的偏好和集中以及行业内小规模兼并收购事件预示着行业逐渐走向集中，马太效应初步显现。

兼并收购趋于频繁

关于数观天下



数观天下是一家专注于数据分析、行业讨论的互联网自媒体，现已为互联网企业、电商、零售、教育、医疗、金融等多个领域进行数据分析。

未经允许，不得对本报告进行改造和加工。如有转载或引用，需及时与我们联系并标明出处。